第三章 同余式

3.1 基本概念及一次同余式

1. 设 m 是一个正整数，$f(x)=a_n x^n+\cdots+a_1 x+a_0$，其中 a_i 是整数，有 $f(x)\equiv 0 \pmod m$ 叫做模 m 同余式.

若 $a_n \not\equiv 0 \pmod m$，则 n 叫做 $f(x)$ 的次数，记为 $\deg f$.

$f(x)\equiv 0 \pmod m$ 叫做模 m 的 n 次同余式.

若有 $x=a$，满足 $f(a)\equiv 0 \pmod m$，则 a 为该同余式的解.

则 $x\equiv a \pmod m$ 都满足，$a\in C_a=\{c \mid c\in\mathbb{Z}, c\equiv a \pmod m\}$

模 m 的完全剩余系中成立的剩余个数叫同余式的解数.

例：$x^5+x+1\equiv 0 \pmod 7$

首项为1的模7的5次同余式

$x\equiv 2 \pmod 7$ 1个解

$f(2)=2^5+2+1=35=5\times 7\equiv 0 \pmod 7$

$x\equiv 4 \pmod 7$ 2个解

$f(4)=4^5+4+1=1029=147\times 7\equiv 0 \pmod 7$

同余式的解数为2.

故本章任务为求解同余式：① $f(x)\pmod p \Rightarrow f(x)\pmod{p^\alpha} \Rightarrow f(x)\pmod m$

② 解的存在性.

③ 解的个数

④ 具体求解.

2. 一次同余式.

$(a,m)=1$，$ax\equiv 1 \pmod m$

$\Downarrow$

$(a,m)=1$，$ax\equiv b \pmod m$

$\Downarrow$

$ax\equiv b \pmod m$

① $m\nmid a$，则 $ax\equiv 1 \pmod m$ 有解的充要条件为 $(a,m)=1$

且解个数一.

//

证：充分性

∵ $(a,m)=1$ ∴ 有 $s\cdot a+t\cdot m=1$ 唯一线性组合

∴ $x=s$ 为同余式的解

必要性

∵ $ax\equiv 1 \pmod m$

∴ 存在 $ax+tm=1$ ∴ $(a,m)=1$

3. m 为正整，a 为整，若存在 a'，使得

$$a'\cdot a\equiv a\cdot a'\equiv 1 \pmod m \text{ 成立}$$

则 a 叫做模 m 可逆元，

由2同理可证，有 a' 唯一，a' 叫做 a 的模 m 逆元

记作 $a'=a^{-1} \pmod m$

∴ 同余式 $ax\equiv 1 \pmod m$ 的解可写成 $x=a^{-1} \pmod m$

4. 给出模简化乘法的一个等价描述。

m 为正整，则 a 是模 m 简化乘法 $\xleftrightarrow{\text{充要}}$ 整数 a 是模 m 逆元。

则有 $(a,m)=1$ 即 $aa'\equiv 1 \pmod m$

可逆元与逆元是相对的

证明已经给出，无需多言

更进步

5. m 为正整，$m\nmid a$，则 $ax\equiv b \pmod m$ 有解

充要

$(a,m)\mid b$

小证一下：$(a,m)=b'$，$b'\mid b$

$s\cdot a+t\cdot m=b'$

$\pmod m$

$s\cdot a\equiv b' \pmod m$

这不是了这个，要 b 是多少 x 就能补上这个倍数。

解 $x \equiv \frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)} \right)^{-1} \pmod{\frac{m}{(a,m)}} \right) + t \cdot \frac{m}{(a,m)} \pmod{m}$

Stop! 我们慢慢看 X!

刚刚证的存在, 只能证求出一个特解. 重来.

证明: 必要性.

设有解 $x \equiv x_0 \pmod{m}$, 即存在 y_0 有 $ax_0 - my_0 = b$

x_0 为一个特殊解

$\because (a,m) \mid a$, $(a,m) \mid m$

$\therefore$ 有 $(a,m) \mid ax_0 - my_0$ 即 $(a,m) \mid b$

证得 有解 $\Rightarrow (a,m) \mid b$

充分性.

设 $(a,m) \mid b$, 则 $\frac{b}{(a,m)}$ 为整数

$\because \left(\frac{a}{(a,m)}, \frac{m}{(a,m)} \right) = 1$

$\therefore$ 由2.得 $x_0 \equiv \left(\frac{a}{(a,m)} \right)^{-1} \pmod{\frac{m}{(a,m)}}$ 有唯一解 x_0

构造 $\frac{a}{(a,m)} x \equiv 1 \pmod{\frac{m}{(a,m)}}$ ⇔ x_0 的唯一

又$\because$ 可以写出 $\frac{a}{(a,m)} x \equiv \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}}$ ⇔

的唯一解 $x \equiv (x_1) \equiv \frac{b}{(a,m)} \cdot x_0 \pmod{\frac{m}{(a,m)}}$ 唯一

↑到这儿好理解

又$\because x \equiv x_1 \equiv \frac{b}{(a,m)} \cdot x_0 \pmod{m}$ 是 $ax \equiv b \pmod{m}$ 的一个特解.

x_1 满足 $\frac{a}{(a,m)} x \equiv \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}}$

则 x_1 是 $ax \equiv b \pmod{m}$ 的一个特解?

同乘 (a,m), 得 $ax \equiv b \pmod{m}$, 前面同等有证.

因此 x_1 是一个特解

∴全部解为 $X \equiv X_1 + t\frac{m}{(a,m)} \pmod m$, $t=0,1,\cdots,(a,m)-1$

用小的把大的(m)中的表示全了就构成了一个乘1余系.

来吧,实战一下.

例. 求 X, $33X \equiv 22 \pmod{77}$

$a=33$, $b=22$, $m=77$

$(a,m)=(33,77)=11 \mid b$

$\frac{a}{(a,m)}=\frac{33}{11}=3$, $\frac{b}{(a,m)}=\frac{22}{11}=2$

$\frac{m}{(a,m)}=\frac{77}{11}=7$

求 X_0, 有 $\frac{a}{(a,m)}X_0 \equiv 1 \pmod{\frac{m}{(a,m)}}$

即 $3X_0 \equiv 1 \pmod 7$, 得 $X_0 \equiv 5 \pmod 7$ (特解)

∴特解 $X_1 \equiv X_0 \cdot \frac{b}{(a,m)} \equiv 5 \cdot 2 \equiv 10 \pmod{\frac{m}{(a,m)}=7}$ (3)

∴ $aX \equiv b \pmod m$ 的解 $X \equiv 10 + 7t \pmod{77}$

$t=1,\cdots,(33,77)-1$

即 $X=3,10,17,24,31,38\cdots,73 \pmod{77}$

3.2 中国剩余定理

离散学过,这里就简单看一下吧.

1. 定理内容: 设 $m_1,\cdots,m_k$ 是 k 个两两互素的正整数,则对任意的整数 $b_1,\cdots,b_k$, 同余式组 $\begin{cases} X \equiv b_1 \pmod{m_1} \\ \vdots \\ X \equiv b_k \pmod{m_k} \end{cases}$

一定有解，且解唯一.

令 $M = m_1 \cdots m_k$

$M_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$

则解 $x = b_1 \cdot M_1 \cdot M_1' + b_2 \cdot M_2 \cdot M_2' + \cdots + b_k \cdot M_k \cdot M_k'$

例：解 $\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 6 \\ x \equiv b_3 \pmod 7 \\ x \equiv b_4 \pmod{11} \end{cases}$ ∵ 5, 6, 7, 11 两两互素

∴ $M = 5 \times 6 \times 7 \times 11 = 2310$

$\begin{cases} M_1 = 2310/5 = 462 \\ M_2 = 2310/6 = 385 \\ M_3 = 2310/7 = 330 \\ M_4 = 2310/11 = 210 \end{cases}$

再求 $\begin{cases} M_1' = 3 \\ M_2' = 1 \\ M_3' = 1 \\ M_4' = 1 \end{cases}$

∴ $x = 3b_1 \cdot 462 + b_2 \cdot 385 + b_3 \cdot 330 + b_4 \cdot 210$

别忘了 $\pmod M$

2. 解 x_i 满足递归 → 废话，有点要再看吧.

$x_i \equiv x_{i-1} + [(b_i - x_{i-1}) M_{i-1}' \pmod{m_i}] \cdot M_{i-1} \pmod{m_1 m_2 \cdots m_i}$

↳ $M_i = m_1 \cdots m_i$，$M_i' M_i \equiv 1 \pmod{m_{i+1}}$

表示为对应之组数据的解

3. 定理的应用 —— 算法优化

① 计算 $2^{1000000} \pmod{77}$

i) 硬算：$2^6 = 256$ 231

$2^7 = 128$ 154

$2^8 = 64$ 77

没规律

ii) $(2, 77) = 1$ $2^{\varphi(77)} \equiv 1 \pmod{77}$ 用欧拉定理

但77不是素数，
求φ(77)也比较麻烦

欧拉有个很好用的性质，$\varphi(77)=\varphi(7)\times\varphi(11)$
$=6\times10=60$

$\therefore 2^{60}\equiv 1 \pmod{77}$

$1000000 \bmod 60 = 40 \bmod 60$

$\therefore 2^{1000000}\equiv 2^{40} \pmod{77}$

~~暴力算~~

用快速幂重复平方.

$40=2^3+2^5$

$n_0=0,\ a_0\equiv 1,\ b_1\equiv 2^2\equiv 4 \pmod{77}$

$n_1=0,\ a_1=a_0=1,\ b_2=b_1^2\equiv 16 \pmod{77}$

$n_2=0,\ a_2=a_1=1,\ b_3=b_2^2=25 \pmod{77}$

$n_3=1,\ a_3=a_2\cdot b_3=25,\ b_4=b_3^2=9 \pmod{77}$

$n_4=0,\ a_4=a_3=25,\ b_5=b_4^2=4 \pmod{77}$

$n_5=1,\ a_5=a_4 b_5=23 \pmod{77}$

$\therefore 2^{1000000}\equiv 2^{40}\equiv 23 \pmod{77}$

~~采用~~中国剩余定理优化：

令 $X=2^{1000000}$

$\because 77=7\cdot 11$ $\therefore$ 求 $X \pmod{77}$ 等价于解方程

$$\begin{cases} X\equiv b_1 \pmod 7 \\ X\equiv b_2 \pmod{11} \end{cases}$$

易得 $2^{1000000}\equiv 2^4\equiv 2 \pmod 7$

$2^{1000000}\equiv 1 \pmod{11}$

解 $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod{11} \end{cases}$ $M = 7 \times 11 = 77$

$M_1 = 11,\ M_2 = 7$

$M_1' \cdot 11 \equiv 1 \pmod 7$ 解得 $M_1' = 2$

$M_2' \cdot 7 \equiv 1 \pmod{11}$ 解得 $M_2' = 8$

$\therefore x \equiv 11 \times 2 \times 2 + 7 \times 8 \times 1 \equiv 100 \equiv 23 \pmod{77}$

因此，$2^{1000000} \equiv 23 \pmod{77}$ ← 好好理解.

② 计算 $312^{13} \pmod{667}$

令 $x = 312^{13}$

$667 = 23 \times 29$ 互素，计算 $\begin{cases} x \equiv b_1 \pmod{23} \\ x \equiv b_2 \pmod{29} \end{cases}$

↓ 用模重复平方法得

$\begin{cases} x \equiv 8 \pmod{23} \\ x \equiv 4 \pmod{29} \end{cases}$

再用中国剩余得 $x \equiv 466 \pmod{667}$

③ 用RSA对math加解密. P106

↳ 假期再进行总结

4. 对于同余式组 $\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$

若 $b_1, b_2, \cdots b_k$ 分别遍历模 $m_1, m_2, \cdots, m_k$ 的完全剩余系

则 $x = b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \pmod m$

也遍历 $m = m_1 \cdot m_2 \cdots m_k$ 的完全剩余系.

思想都大同小异，不证明了.

5. 设 $m_1, \cdots, m_k$ 为 k 个互素正整.

$M = m_1 \cdots m_k$

存在唯一的一组 b_i，有

证明思路可以参考中国剩余定理的应用——算法优化那一节集锦.

$x = b_1 \cdot M_1' \cdot M_1 + \cdots + b_k \cdot M_k' \cdot M_k \equiv b \pmod M$

$\Downarrow$

$(b, M) = 1 \Leftrightarrow (b_i, m_i) = 1$ （充要）

3.3 高次同余式的解数及解法

1. 高次同余式的解数. → 3.3学会这个就行了

① $f(x) \equiv 0 \pmod m$

与同余式组 $\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ \vdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases}$

$m = \underbrace{m_1 \cdot m_2 \cdots m_k}_{\text{互素}}$

等价.

证明：若 $f(x_0) \equiv 0 \pmod m$

由于 $m = m_1 \cdot m_2 \cdots m_k$

$\therefore f(x_0) \equiv 0 \pmod{m_i}$

若有 $f(x_0) \equiv 0 \pmod{m_i}$ 第二章同余的知识

由定理 $a \equiv b \pmod{m_i}$ 且 $a \equiv b \pmod{[m_1, \cdots m_k]}$

得 $f(x_0) \equiv 0 \pmod m$

故证得两者解等价.

② 已经证明了两者解等价

设 $\begin{cases} x \equiv b_1 \pmod{m_1} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$ 解为 $x \equiv b_1 \cdot M_1' \cdot M_1 + \cdots + b_k \cdot M_k' \cdot M_k \pmod m$

可以一直加 m_1

$\therefore f(x) \equiv f(b_i) \equiv 0 \pmod{m_i}$

x 随着 b_i 遍历 $f(x) \equiv 0 \pmod{m_i}$ 的所有解而遍历 $f(x) \equiv 0 \pmod m$ 的所有解.

$\therefore$ 解数 $T = T_1 \cdots T_k$

罢了，我们直接着题理解吧.

例：解同余式 $f(x)\equiv x^4+2x^3+6x+9\equiv 0 \pmod{35}$

等价于 $\begin{cases} f(x)\equiv 0 \pmod 5 \\ f(x)\equiv 0 \pmod 7 \end{cases}$

直接求解，（因为5,7值很小，$x=1,2,3,4,5,6,7$都带进去也花不了多长时间）

$f(x)\equiv 0 \pmod 5$ 的解为 $x\equiv 1,4 \pmod 5$

$f(x)\equiv 0 \pmod 7$ 的解为 $x\equiv 3,5,6 \pmod 7$

根据中国剩余定理，可求得同余式组

$\begin{cases} x\equiv b_1 \pmod 5 \\ x\equiv b_2 \pmod 7 \end{cases}$ 代入 b_1, b_2

解为 $x\equiv 21b_1+15b_2 \pmod{35}$

为什么要有这一步？

因为求出来后 x 的值应该是统一的，因此再通过中国剩余统一出一个解来。

$\therefore x=31,21,6,24,19,34 \pmod{35}$ 解有 $2\times 3=6$ 个。

2. 高次同余式的提升

$f(x)\equiv 0 \pmod{p^\alpha}$ 其中 p 为素数

$m=\prod p^\alpha$ 任意一正整数 m 有特性素数分解式

则要求 $f(x)\equiv 0 \pmod m$

只需求 $\begin{cases} f(x)\equiv 0 \pmod{p^\alpha} \\ \text{组} \quad \vdots \end{cases}$

设 $f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0$

则 $f'(x)=n\cdot a_n x^{n-1}+\cdots+2a_2x+a_1$

有定理：设 $x\equiv x_1 \pmod p$ 是同余式

$f(x)\equiv 0 \pmod p$ 的一个解，且

$(f'(x_1),p)=1$

则 $f(x)\equiv 0 \pmod{p^\alpha}$ 有解 $x\equiv x_\alpha \pmod{p^\alpha}$

（x_α 可以通过一个超复杂的递归得到，证明这个递归更复杂，这里字太多省了）

⇓ 保护自己最重要～ 书P111-113

3. 高次同余式的提升 —— 具体应用

例：求解同余式 $f(x)\equiv x^4+7x+4\equiv 0 \pmod{27}$

参P113-115，相当神奇相当炫酷！

3.4 素数模的同余式

探究如何求解模素数p的同余式

$$f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0 \pmod p \qquad a_n\not\equiv 0 \pmod p$$

1. 素数模的多项式欧几里得除法

$f(x)$为n次整系数多项式

$g(x)=x^m+\cdots+b_1x+b_0$为$m\geq 1$次首一整系数多项式

则存在整系数多项式$q(x)$和$r(x)$使得

$$f(x)=q(x)\cdot g(x)+r(x),\quad \deg r(x)<\deg g(x)$$

我的平价是这个东西贯穿高中数学

证明：(i) $n<m$时，取$q(x)=0$，$r(x)=f(x)$，成立

(ii) $n\geq m$时，对$f(x)$的次数n作数学归纳.

当$n=m$时，有 $f(x)-a_n\cdot g(x)=(a_{n-1}-a_n\cdot b_{m-1})x^{n-1}+\cdots+(a_1-a_n\cdot b_0)x+a_0$

$\therefore q(x)=a_n$，$r(x)=f(x)-a_n\cdot g(x)$，成立

假设$n-1\geq m$时，结论成立.

对于$n>m$，有

$$f(x)-a_nx^{n-m}g(x)=\underline{(a_{n-1}-a_n\cdot b_{m-1})x^{n-1}+\cdots(a_{n-m}-a_n\cdot b_0)x^{n-m}}+a_{n-m-1}x^{n-m-1}+\cdots+a_0$$

到这儿$g(x)$已经用完了.

这说明$f(x)-a_nx^{n-m}\cdot g(x)$是次数为$\leq n-1$的多项式.

故存在$q_1(x)$和$r_1(x)$，使

$$f(x)-a_nx^{n-m}\cdot g(x)=q_1(x)\cdot g(x)+r_1(x),\quad \deg r_1(x)<\deg g(x)$$

$\therefore q(x)=a_nx^{n-m}+q_1(x)$，$r(x)=r_1(x)$成立.

综上，证得 $f(x)=q(x)\cdot g(x)+r(x)$，$\deg r(x)<\deg g(x)$

首一整系数

2. 素数模的同余式的简化

① $x^p\equiv x \pmod p$ 对于任何整数 x 取值为 0（费马定理）

+ 素数

② 多项式欧几里得除法

= 将高次多项式化为不超过 $p-1$ 次

$f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0 \pmod p$

与一个不超过 $p-1$ 的模 p 同余等价

素

证明：存在 $q(x)$，$r(x)$，使得

$f(x)=q(x)(x^p-x)+r(x)$　　$\deg r(x)\le p-1$

又：$x^p-x\equiv 0 \pmod p$

∴ 同余式 $f(x)\equiv 0 \pmod p$ 等价于

$r(x)\equiv 0 \pmod p$

例. 求与同余式 $f(x)=3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\equiv 0 \pmod 5$

∴令 $g(x)=x^5-x\equiv 0 \pmod 5$

作欧几里得除法，有

$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x$

$=(3x^9+4x^8+2x^6+5x^4+2x^2+4x+5)(x^5-x)+3x^3+16x^2+6x$

怎么化的呢？

$r_0(x)=f(x)-3x^9\cdot g(x)=4x^{13}+2x^{11}+3x^{10}+x^9+x^6+x^3+12x^2+x$

$r_1(x)=r_0(x)-4x^8g(x)$

⋮

一直减到最高次 $\le p-1=4$

∴ 原式等价于 $r(x) = 3x^3 + 16x^2 + 6x \equiv 0 \pmod 5$

直接取 $x = 0, 1, 2, 3, 4$ 得 $x \equiv 0, 1, 2 \pmod 5$

3. 素数模的同余式的因式分解

同余式的解数不大于其次数.

① 设 $1 \le k \le n$, 若

$$x \equiv a_i \pmod p, \quad i = 1, \cdots, k$$

是 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p$ 的 k 个不同解, 则有

$$f(x) \equiv f_k(x) \cdot (x - a_1) \cdots (x - a_k) \pmod p$$ 对任意 x 成立.

其中 $f_k(x)$ 是 $n-k$ 次多项式, 首项系数是 a_n

证明: 由欧几阵得存在 $f_1(x)$ 与 $r(x)$, 有

$$f(x) = f_1(x) \cdot (x - a_1) + r(x), \quad \deg r(x) < \deg (x - a_1)$$

易知 $\deg f_1(x) = n-1$, 首项为 a_n, $r(x) = r$ 为整数.

$\because f(a_1) \equiv 0 \pmod p \quad \therefore r \equiv 0 \pmod p$

$\therefore f(x) \equiv f_1(x) \cdot (x - a_1) \pmod p$ (与 p 互素)

又 $\because f(a_2) \equiv 0 \pmod p$ 且 $a_2 \not\equiv a_1 \pmod p$

$\therefore f_1(a_2) \equiv 0 \pmod p$

$i = 2, \cdots, k$.

怎么来的得到?

已知 $(x - a_1) \not\equiv 0 \pmod p$

会得到一个位于 p 的完全剩余中的值. (p 为素数)

因此 $f_1(x) \cdot (x - a_1) \pmod p = 0$

只有 $f_1(x) \equiv 0 \pmod p$

没有能补上 $(x - a_1)$ 的变为 0.

剩余类里两个质元配不出来, 符能配 0 出来, 首先因.

多理解!

类似的, 还可以得到

$$\begin{cases} f_1(x) \equiv f_2(x) \cdot (x - a_2) + r_2(x) \\ f_2(a_i) \equiv 0 \pmod p, \ i = 3, \cdots, k \end{cases}$$ 得 0

↓ 一直往下, 有

$$f_{k-1}(x) \equiv f_k(x)(x - a_k) \pmod p$$

$\therefore$ 有 $f(x) \equiv f_k(x)(x - a_1) \cdots (x - a_k) \pmod p$

例. $(3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x) \pmod 5$

上面做法. 解为 $x=0,1,2 \pmod 5$

$\equiv x(x-1)(x-2)(3x^{11}+3x^{10}+3x^9+4x^7+3x^6+x^5+2x^4+x^2+3x+3) \pmod 5$

② p为素数. 有 ⇓ 求证

i) 任意整x, $x^{p-1}-1 \equiv (x-1)\cdots[x-(p-1)] \pmod p$

$x^{p-1} \equiv 1 \pmod p$ → 欧几里得 回顾书P6

故 $f(x)=x^{p-1}-1 \equiv 0 \pmod p$

所有解为 $1 \sim p-1$

少了个 $f_k(x)$ 没了. 除了 $p-1$ 个 x, $f_k(x)$ 已经无了.

ii) Wilson定理 $(p-1)! \equiv -1 \pmod p$

即 $(p-1)!+1 \equiv 0 \pmod p$

n为素数 ⇔ (充要) $(n-1)!+1 \equiv 0 \pmod n$ ☆

半: 断是否为素数很好用!

4. 素数模的同余式的解数估计.

1说了 $f(x)=q(x)\cdot g(x)+r(x)$

2说了 把 $f(x)$ 简化为 $r(x)$

3说了 $f(x)$ 能因式分解 ↓

4 我们就要讨论 $f(x)$ 的解的个数了.

上界: ①不超过它的次数 → 懂得都懂

② $f(x)=x^n+\cdots+a_1x+a_0 \equiv 0 \pmod p$ (p 素数)

若 $n \le p$. 则有 n 个解 ⇔ (充要) (x^p-x) 被 $f(x)$ 除 所得式所有系数都是 p 的倍数

为什么?, 因为 p 为素, 只有 $0 \sim p-1$ 共 p 个.

有 $f(x)=q(x)(x^p-x)+r(x)$ 系数

也有 $x^p-x=q(x)\cdot f(x)+r(x)$ 都是p倍数

$n\le p$

上例子！

例1：判断 $2x^3+5x^2+6x+4\equiv 0 \pmod 7$ 是否有三个解

① 变 $f(x)$ 为首1

$4(2x^3+5x^2+6x+4)\equiv x^3-x^2+3x-3 \pmod 7$

② 有 $x^7-x\equiv x(x^3+x^2-2x-2)\cdot(x^3-x^2+6x-3)+7x(x^2-1)$

$r(x)$

$7x^3-7x$

所有系数都是7的倍数

∴有3个解.

例2：求解 $21x^{15}+2x^{15}-x^{10}+4x-3\equiv 0 \pmod 7$

① 次数太大，化简 $7\mid 21$ ？

$2x^{15}-x^{10}+4x-3\equiv 0 \pmod 7$

怎么得这个式子再看看书 P117 上面.

$2x^{15}-x^{10}+4x-3=(2x^8-x^5+2x^2)(x^7-x)+(-x^4+2x^3+4x-3)$

得等价同余式 $x^4-2x^3-4x+3\equiv 0 \pmod 7$

写全算 $x=0,\pm1,\pm2,\pm3$ 了解决上面更好

$0,1,2,3,-4,-5,6$

例3：$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\equiv 0 \pmod 5$

解法一：欧几里得降法化简，同2.

解法二：费马小定理，欧拉！ 直接得到了！

5为素数，有 $x^4\equiv 1 \pmod 5$

因此 原式 $\equiv 3x^2+4x+2x^3+x+x^2+x^3+12x^2+x$

$\equiv 3x^3+16x^2+6x\equiv 0 \pmod 5$

再代入 $0,\pm1,\pm2$ 检验.